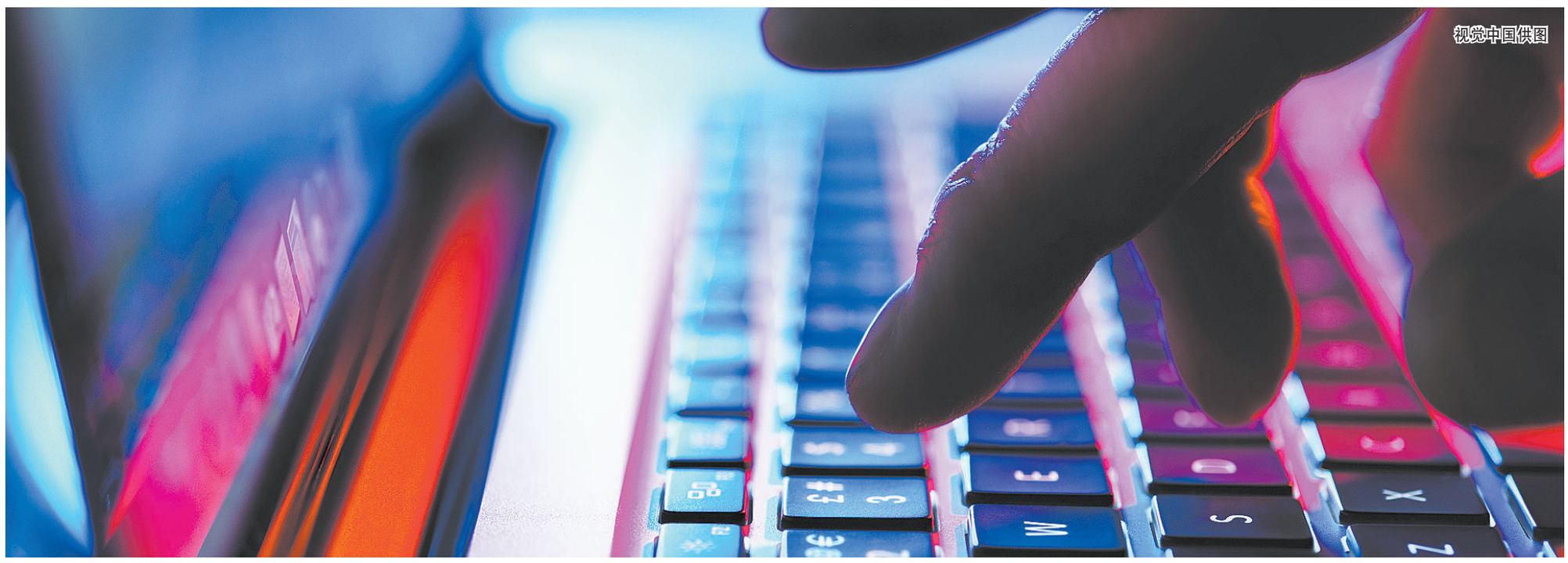
骗术随技术「进化」 反击电信网络诈骗胜算几何


视觉中国供图

深瞳工作室出品

采 写：本报记者 崔 爽
策 划：刘 莉

“账户有风险，请核实对方真实身份后再转账。”

10月11日，2021国家网络安全宣传周活动在西安启动，同期举办的网络安全博览会上，交互模拟产品“反诈盲盒”吸引了很多人驻足体验。

打开这个盲盒，体验者收获了一位网上掉出来的“男朋友”。这个“男朋友”用甜言蜜语诱你转账，虽然只有2分钱，但支付宝仍通过弹窗提示、防骗试卷等方式加以阻止，AI客服甚至花了超过5分钟时间，“苦口婆心”劝阻。

人工智能等新技术正在成为“反诈利器”。但与此同时，让人无奈的是它也让骗子更强了。

当人们把越来越多的生活场景搬上网络，互联网上的安全也变得越发重要。诈骗和反诈像一场没有硝烟的战争，旷日持久，变化莫测：90后成受骗重灾区、诈骗“产业链”越发完备、诈骗也能“技术外包”……

处理好安全与发展的关系，在网络世界同样成为我们必须面对的议题。习近平总书记今年对打击治理电信网络诈骗犯罪工作作出重要指示，强调要以人民为中心，统筹发展和安全，强化系统观念、法治思维，注重源头治理、综合治理，坚持齐抓共管、群防群治，全面落实打防管控各项措施和金融、通信、互联网等行业监管主体责任，加强法律制度建设，加强社会宣传教育防范，推进国际执法合作，坚决遏制此类犯罪多发高发态势。

诈骗没有“免疫人群” 九零后是受骗重灾区

高学历、有一定经济基础的人群也不能对网络诈骗“免疫”

如果让你给网诈受害者画像，你觉得他们是什么样？

精神空虚、爱占小便宜、缺乏判断力是“易受骗体质”的特性？事实上，他们中的大多数人年轻、受良好教育、谙熟互联网。

作为互联网原住民的90后、00后，正在成为诈骗团伙的主要目标。

中国信息通信研究院和360联合发布的《2020年中国手机安全状况报告》显示，在网络诈骗举报用户中，90后的手机诈骗受害者占所有受害者总数的37.5%，是不法分子从事网络诈骗的主要受众人群；其次是00后，占比为28.7%。而印象中更容易遭受诈骗的70后和60后人群，仅占比不到10%。

上海市公安局也曾披露，全市接报的电信网络诈骗既遂案件中，1990年以后出生的受害人数量占比超过六成。

前段时间，有媒体发布消息，他们一位编发过无数电信诈骗新闻的90后编辑，被“冒充公检法”的诈骗手段骗走5万元。

对方自称“警方”，称他涉嫌洗钱，要把其名下财产转移到“安全账户”。在骗子的话术控制下，他不仅把自己账户上的近3万元转走，甚至去线上借贷平台贷款了近2万。


视觉中国供图

据其事后总结，对方的骗术其实并不高明，避开陷阱的机会也不少：不要随意接号码奇怪的陌生电话，不要相信公安机关的电话会被转接，不要相信所谓的“安全账户”……但一时大意、鬼使神差，新闻人成了新闻当事人。

“很多人认为年龄偏大、文化水平偏低的人群最容易遭遇网络诈骗，实际上，高学历、有一定经济基础的人群也并非网络诈骗的‘免疫人群’。”刑科协反诈专委会筹备办主任胡永涛介绍，“随着网络诈骗逐渐成为主流，受骗人群越来越呈现年轻化的趋势。”

他表示，总体来看，在受害群体中占比最高的是18至40岁的人群，90后、00后是诈骗分子的“重点关照对象”，占比最高的诈骗类型有刷单刷信誉、网络贷款、投资理财、冒充购物客户退款、冒充熟人诈骗等。据不完全统计，90后是受骗重灾区，受骗数量超过其他年龄段人数总和，占比达63.7%。

根据上海警方发布的数据，在90后、00后等群体遭遇的电信网络诈骗既遂案件中，兼职刷单类占24.7%、网购类占23.2%、冒充客服类占13.2%、“杀猪盘”类（利用网络交友诱导受害人投资赌博的一种电信诈骗）占12.1%。这些诈骗手法并不新奇，却足以把涉世未深的年轻人甚至未成年人引入圈套。

> 互联网产业迅猛发展，更加速了犯罪手法和手段的变化，往往网络新技术新业态一出现，利用其实施的电信网络诈骗随之产生。当前，网络诈骗与反诈的技术对抗处于焦灼状态，基本上每破解一道骗术，犯罪分子技术手段就会升级。

网诈也有“产业链” 正邪技术对抗焦灼

骗术不断翻新，诈骗“产业链上下游”也在“进化”

进行网络诈骗的，到底是一群什么样的人？

“撬开人们的钱袋子并不容易。”黑猫曾是一名警察，如今是“守护者计划”安全专家，他发现，很多诈骗公司早已发展出一套包括思想课、技术课、角色扮演等在内的完整“培训流程”。他们自行编写动辄一百多页的“剧本”，传授行骗话术，集团成员还要进行角色扮演，模拟对战。

骗子编写剧本时，甚至会考虑用户不同程度的警戒心与消极反应，设置不同方案来瓦解对方心理防线。比如触发紧张情绪，也要兼顾风土人情、时令节气，自然说出台词——春运期间多进行票务诈骗；黄金周前主要用“护照申请”诈骗；对北方人讲话通常开门见山，对南方人要讲究条理与逻辑。

在安装了吸音海绵的工作间里，话务员每人每天至少要打300通有效电话，每次通话30秒以上。这意味着一个20人左右的犯罪团伙，每天甚至能输出近一万通电话。

除了不断翻新的骗术，诈骗的“产业链上下游”也在“进化”。

“十年前，电信诈骗有一定门槛。在境外建设窝点，可能需要两百万元投入，而且要懂点技术。而现在，只要一个人、一台电脑就够了，其他外包给‘专业人士’——引流推广、养号、支付渠道、洗钱……各式网络犯罪看不见摸不着，却发展出一条完整产业链，统称‘黑灰产’。”“守护者计划”安全专家晓树介绍说。

2016年，刚刚考上大学的18岁女孩徐玉玉因遭遇电信诈骗离世，引发舆论震动。同年，腾讯公司发起政企联合反诈骗公益平台“守护者计划”，成立了首个反诈骗实验室，依托其安全大数据、底层技术和海量用户优势，协同社会多方力量，旨在为民众提供全方位的网络安全防护。

对战多年，晓树谈到骗子的“与时俱进”：打电话这种体力活早已被交给机械化运行的机器群呼，“号商”采取公司化运作，批量获取大量账号、密码和公民个人信息。

去年3月28日，西安碑林警方曾披露一起非法提供“群呼”设备的案件：他们摸排发现辖区存在一个绑载了多个手机号码的GoIP设备窝点，可能涉及多起全国各地电信网络诈骗案件。据了解，GOIP设备是一种具备多条线路并可配备多个手机SIM卡卡槽、支持手机电话卡接入并将传统电话信号转化为网络信号、实现数百个电话号同时通话的设备。

类似设备只需要宽带连接，就可以用电脑控制。“都是远程操控，设备在境内，真正实施诈骗的团伙却躲在境外，这也是电信诈骗案侦破难的主要原因。”当地警方介绍，被打掉的团伙给境外诈骗团伙提供“技术支持”。

仅在被打掉前8天，通过架设的GoIP设备，境外多个诈骗团伙就先后呼出了10多万个诈骗电话，其中成功实施诈骗130多起，“效率”之高可见一斑。

“当前，网络诈骗犯罪呈现精准化、组织化、专业化趋势，催生了为诈骗犯罪提供帮助和支持，并从中获利的黑灰产，成为滋生网络诈骗的温床。”胡永涛说，他们研究发现，网络诈骗犯罪已经形成由养号租号买卖、打码接码推广、技术团队运营、话术脚本编制以及洗钱通道所构建的链条式黑灰产组织，加速了网络诈骗犯罪的蔓延泛滥。

“底层是基础技术环节，比如验证码识别、自动化软件开发、钓鱼网站制作等；中层则是一些账号、用户信息提供商，组织、运营和推广诈骗活动，发展下线；再往上，就是进行诈骗活动者，利用窃取的信息、账号和诈骗工具等开展包括欺诈、盗窃、钓鱼等诈骗行为，实现获利。”志翔科技高级副总裁伍海桑进一步解释。

去年，“杀猪盘”异军突起，成为受害者损失金额最高的诈骗类型。靠这种打着爱情旗号的新型诈骗手段，三五人的小团伙就能将800多人坑害成“猪仔”，涉案金额超过两亿元。

互联网产业迅猛发展，更加速了犯罪手法和手段的变化，往往网络新技术新业态一出现，利用其实施的电信网络诈骗随之产生。“当前，网络诈骗与反诈的技术对抗处于焦灼状态，基本上我们每破解一道骗术，犯罪分子技术手段就会升级。”工信部反诈中心主任、中国信息通信研究院副院长魏亮语带无奈。

胡永涛表示，据不完全统计，近年来公安机关打击的诈骗类型已有50种以上。近两年，作案手法出现了从电话、短信向网络发展的新动向，网络诈骗案件占比迅速上升，达到80%以上，其中网络贷款、网络刷单、网络购物、网络投资等诈骗发案最多。

明确权责社会共治 对抗黑灰产需群策群力

构建群防群治机制，还需加强组织协调

打击网络诈骗到底难在哪儿？

偷窃不成功，可能进牢房。抢劫不成功，可能被暴揍。诈骗不成功？换个电话接着来。

段子虽属调侃，背后却暗含网络诈骗屡禁不绝的主因。胡永涛直言：违法成本低、处置障碍大、轻罪惩戒难。

他表示，滋生网络黑灰产的核心原因是“人（账）户分离”，特别是推广链、资金链中广泛出现的租/售电话卡、银行卡、网络账号行为，帮助犯罪分子以他人实名账户、账号为掩护躲避公安机关追查、构建诈骗场景，以较小的违法成本，增加了防范打击的难度。更棘手的是，黑灰产人员租售网络账户，违法所得有时不够立案标准，部分黑灰产人员长期从事相关违法活动，积累了大量对抗和反侦查经验，开始搭建黑灰产技术平台，为境外网络诈骗犯罪提供专业化支持。

“守护者计划”安全专家周克提到，在东南亚某地，有电信器材店专门服务于犯罪团伙，职业HR以正规人力资源的招聘流程，拐骗刚毕业的大学生担任黑灰产程序员。他们实力雄厚，有的能为“员工”开出数万元月薪，提供新冠疫苗等“福利”。诈骗团伙的“蓬勃发展”甚至令当地房价水涨船高。

“估计参与黑灰产的人数达百万，而正义一方连对方人数的十分之一都不到。”周克说。

不过，经过多年机器训练，目前，大数据、人工智能已能逐渐自行寻找平台上的诈骗风险。周克和同伴们相信，凡诈骗必留下痕迹，无论通过电话、短信、钓鱼网址还是外挂软件，这些痕迹会成为大数据的一部分，数据量越大，分析技术越强，对于电信网络诈骗的预防、发现和打击越精准有效，“这是不可违背的定律”。

今年5月，工信部启动“断卡2.0”专项行动。7月14日，12381涉诈预警劝阻短信系统正式启动，工信部组织建设了信息通信行业反诈大平台，实现对涉案号码、域名、互联网账号等全网一体化处置。

胡永涛强调，反诈是需要各方面社会力量共同参与的综合治理工作，主要包括打击犯罪、预警劝阻、行业治理、宣传防范等。他坦言，要构建群防群治机制，还需加强组织协调，进一步解决信息共享、犯罪预防治理、法规建设等问题。

“我国目前尚未出台针对新型网络犯罪的法律，很多电信网络治理信息共享工作处于无法可依的状态。”胡永涛说，电信网络违法犯罪的治理，涉及公共权力的行使、公共利益的保护、各个企业的风险控制，国家、社会和企业利益与个人信息上所承载的个体权益之间的冲突如何衡量，亟须相应指引和规范。

同时他也提到，一些企事业单位在治理工作中发现的问题和线索，由于没有明确治理权，大量预警线索和信息未能得到充分利用。一方面，由于企业发现的问题往往还未导致案情，或找不到受害人，公安机关很难快速定性并依法处置，另一方面，金融机构、电信运营商、互联网企业对于发现的涉诈线索，无法定性处置，也很难做到自身业务范围以外的联防联控。

这让法规建设、权责明确成为当务之急。“应首先对监管部门、司法部门、金融机构、电信运营商、互联网公司等在反电信网络诈骗中的分工、责任和协同联通机制进行明确，形成治理合力。”胡永涛建议。

“一方面要从法规层面要求互联网服务提供商从技术、责任、道德多方面对于数据安全保护担责；一方面全方位、大力度惩治网诈行为。同时建立公共信息平台，形成信息、宣传、技术的能力聚合与共享，集结安全厂商的能力，更好地服务用户。”伍海桑表示，他特别提到，相关企业应履行社会责任，在法规、标准制定方面积极建言献策。

另外，反诈必须“攻防并举”。公安部刑事侦查局副局长姜国利表示，电信网络诈骗是可防性犯罪，事后打击不如事前的防范，快破案不如不发案，多追赃不如少受骗。

胡永涛同样谈到，由于诈骗团伙大部分躲在境外，加上受疫情影响，公安出境打击此类犯罪的成本非常高。相比之下，开展群防群治工作，可以大大节约社会整体成本，降低群众受骗风险。

大众是“社会共治”的重要力量。如黑猫所说，普通人可以随手标记诈骗电话、短信、网址，及时举报诈骗行为，完善反诈安全数据库，为“全民反诈、天下无诈”出力。

在诈骗与反诈的猫鼠游戏中，每个人都可能是受害者，也都可以是行动派。

（文中黑猫、晓树、周克均为化名）

相关链接

探索社会共治新模式 反诈专委会将成立

◎本报记者 崔 爽

电信网络诈骗治理环节众多，分属不同监管部门和平台企业，急需进一步厘清权责、形成合力。记者近日从公安部第三研究所获悉，反电信网络诈骗专业委员会（以下简称专委会）正在筹备成立，有望让这一问题迎刃而解。

专委会由国务院打击治理电信网络新型违法犯罪工作部际联席会议办公室指导，设于中国刑事科学技术协会下，由公安部第三研究所牵头50多家知名企事业单位共同发起筹建。专委会将围绕协调共享信息、推动警企合作、交流反诈技术、组织反诈培训、宣传反诈知识等方面展开合作，探索形成有效的技术和业务合作机制，创造健康网络生态的行动共同体，充分发挥委员会成员各自优势，实现反诈信息资源的高效利用，提高反诈工作的效率和质量，压缩涉诈人员的违法活动空间，实现减少电信网络诈骗发案数。